are about Federal personnel must be greater than of any other category).

(ii) The purpose of the match must not be for purposes of taking any adverse financial, personnel, disciplinary, or other unfavorable action against an individual.

(6) Performed using only records from systems of records maintained by an agency.

(i) The purpose of the match must not be for purposes of taking any adverse financial, personnel, disciplinary, or other unfavorable action against an individual.

(ii) A match of DoD personnel using records in a system of records for purposes of identifying fraud, waste, and abuse is not covered.

(7) Performed to produce background checks for security clearances of Federal or contractor personnel or performed for foreign counter-intelligence purposes.

### § 310.52 Computer matching publication and review requirements.

(a) DoD Components shall identify the systems of records that will be used in the match to ensure the publication requirements of subpart G have been satisfied. If the match will require disclosure of records outside the Department of Defense, Components shall ensure a routine use has been established, and that the publication and review requirements have been met, before any disclosures are made (see subpart G of this part).

(b) If a computer matching program is contemplated, the DoD Component shall contact the DPO and provide information regarding the contemplated match. The DoD DPO shall ensure that any proposed computer matching program satisfies the requirements of the Privacy Act (5 U.S.C. 552a) and OMB Matching Guidelines (54 FR 25818 (June 19, 1989)).

(c) A computer matching agreement (CMA) shall be prepared by the Component, consistent with the requirements of § 310.53 of this subpart and submitted to the DPO. If the CMA satisfies the requirements of the Privacy Act (5 U.S.C. 552a) and OMB Matching Guidelines (54 FR 25818 (June 19, 1989)), as well as this subpart, it shall be forwarded to the Defense Data Integrity Board (DIB) for approval or disapproval.

(1) If the CMA is approved by the DIB, the DPO shall prepare and forward a report to both Houses of Congress and to OMB as required by, and consistent with, OMB Circular A–130, ''Management of Federal Information Resources,'' February 8, 1996, as amended. Congress and OMB shall have 40 days to review and comment on the proposed match. Any comments received must be resolved before matching can take place.

(2) If the CMA is approved by the DIB, the DPO shall prepare and forward a match notice as required by OMB Circular A–130, ''Management of Federal Information Resources,'' February 8, 1996, as amended, for publication in the FEDERAL REGISTER. The public shall be given 30 days to comment on the proposed match. Any comments received must be resolved before matching can take place.

### § 310.53 Computer matching agreements (CMAs).

(a) If a match is to be conducted internally within DoD, a memorandum of understanding (MOU) shall be prepared. It shall contain the same elements as a CMA, except as otherwise indicated in paragraph (b)(4)(ii) of this section.

(b) A CMA shall contain the following elements:

(1) *Purpose.* Why the match is being proposed and what will be achieved by conducting the match.

(2) *Legal authority.* What is the Federal or state statutory or regulatory basis for conducting the match. The Privacy Act does not constitute independent authority for matching. Other legal authority shall be identified.

(3) *Justification and expected results.* Explain why computer matching as opposed to some other administrative means is being proposed and what the expected results will be, including a specific estimate of any savings (see paragraph (b)(13) of this section).

(4) *Records description.* Identify:

(i) The system of records or non-Federal records. For DoD systems of records, provide the FEDERAL REGISTER citation for the system notice;

(ii) The specific routine use in the system notice if records are to be disclosed outside the Department of Defense (see §310.22(c)). If records are disclosed within the Department of Defense for an internal match, disclosures are permitted pursuant to paragraph (a) of §310.22.

(iii) The number of records involved;

(iv) The data elements to be included in the match;

(v) The projected start and completion dates of the match. CMAs remain in effect for 18 months but can be renewed for an additional 12 months provided:

(A) The match will be conducted without any change, and

(B) Each party to the match certifies in writing that the program has been conducted in compliance with the CMA or MOU.

(vi) How frequently will the records be matched.

(5) *Records accuracy assessment.* Provide an assessment by the source and recipient agencies as to the quality of the information that will be used for the match. The poorer the quality, the more likely that the program will not be cost-effective.

(6) *Notice procedures.* Identify what direct and indirect means will be used to inform individuals that matching will take place.

(i) *Direct notice.* Indicate whether the individual is advised that matching may be conducted when he or she applies for a Federal benefit program. Such an advisory should normally be part of the Privacy Act Statement that is contained in the application for benefits. Individual notice sometimes is provided by a separate notice that is furnished the individual upon receipt of the benefit.

(ii) *Indirect notice.* Indicate whether the individual is advised that matching may be conducted by constructive notice. Indirect or constructive notice is achieved by publication of a routine use in the FEDERAL REGISTER when the matching is between agencies or is achieved by publication of the match notice in the FEDERAL REGISTER.

(7) *Verification procedures.* Explain how information produced as a result of the match will be independently verified to ensure any adverse information obtained is that of the individual identified in the match.

(8) *Due process procedures.* Describe what procedures will be used to notify individuals of any adverse information uncovered as a result of the match and to give such individuals an opportunity to either explain the information or how to contest the information. No adverse action shall be taken against the individual until the due process procedures have been satisfied.

(i) Unless other statutory or regulatory authority provides for a longer period of time, the individual shall be given 30 calendar days from the date of the notice to respond to the notice.

(ii) If an individual contacts the agency within the notice period and indicates his or her acceptance of the validity of the adverse information, the agency may take final action. If the period expires without a response, the agency may take final action.

(iii) If the agency determines that there is a potentially significant effect on public health or safety, it may take appropriate action notwithstanding the due process provisions.

(9) *Security procedures.* Describe the administrative, technical, and physical safeguards that will be established to preserve and protect the privacy and confidentiality of the records involved in the match. The level of security must be commensurate with the level of the sensitivity of the records.

(10) *Records usage, duplication, and redisclosure restrictions.* Describe any restrictions imposed by the source agency or by statute or regulation on the collateral uses of the records. Recipient agencies may not use the records obtained for matching purposes for any other purpose absent a specific statutory requirement or where the disclosure is essential to the conduct of the matching program.

(11) *Disposition procedures.* Clearly state that the records used in the match will be retained only for the time required for conducting the match. Once the matching purpose has been achieved, the records will be destroyed unless the records must be retained as directed by other legal authority. Unless the source agency requests that the records be returned,

identify the means by which destruction will occur, i.e., shredding, burning, electronic erasure, etc.

(12) *Comptroller General access.* Include a statement that the Comptroller General may have access to all records of the recipient agency to monitor or verify compliance with the terms of the CMA.

(13) *Cost-benefit analysis.* (i) A cost-benefit analysis shall be conducted for the proposed computer matching program unless:

(A) The Data Integrity Board waives the requirement, or

(B) The matching program is required by a specific statute.

(ii) The analysis must demonstrate that the program is likely to be cost-effective. This analysis is to ensure agencies are following sound management practices. The analysis provides an opportunity to examine the programs and to reject those that will only produce marginal results.

## APPENDIX A TO PART 310—SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION (PII)

(See §310.13 of Subpart B)

### A. GENERAL

1. The IT environment subjects personal information to special hazards as to unauthorized compromise, alteration, dissemination, and use. Therefore, special considerations must be given to safeguarding personal information in IT systems consistent with the requirements of DoD Directive 8500.1 and DoD Instruction 8500.2.

2. Personally identifiable information must also be protected while it is being processed or accessed in computer environments outside the data processing installation (such as, remote job entry stations, terminal stations, minicomputers, microprocessors, and similar activities).

3. IT facilities authorized to process classified material have adequate procedures and security for the purposes of this Regulation. However, all unclassified information subject to this Regulation must be processed following the procedures used to process and access information designated ''For Official Use Only.'' (See DoD 5200.1–R.)

### B. RISK MANAGEMENT AND SAFEGUARDING STANDARDS

1. Establish administrative, technical, and physical safeguards that are adequate to protect the information against unauthorized disclosure, access, or misuse. (See OMB Circular A–130 and DoD Instruction 8500.2.)

2. Tailor safeguards to the type of system, the nature of the information involved, and the specific threat to be countered.

### C. MINIMUM ADMINISTRATIVE SAFEGUARDS

The minimum safeguarding standards as set forth in §310.13(b) apply to all personal data within any IT system. In addition:

1. Consider the following when establishing IT safeguards:

a. The sensitivity of the data being processed, stored and accessed.

b. The installation environment.

c. The risk of exposure.

d. The cost of the safeguard under consideration.

2. Label or designate media products containing personal information that do not contain classified material in such a manner as to alert those using or handling the information of the need for special protection. Designating products ''For Official Use Only'' in accordance with the requirements of DoD 5200.1–R satisfies this requirement.

3. Mark and protect all computer products containing classified data in accordance with the requirements of DoD 5200.1–R and DoD Directive 8500.1.

4. Mark and protect all computer products containing ''For Official Use Only'' material in accordance with the requirements of DoD 5200.1–R.

5. Ensure that safeguards for protected information stored at secondary sites are appropriate.

6. If there is a computer failure, restore all protected information being processed at the time of the failure using proper recovery procedures to ensure data integrity.

7. Train personnel involved in processing information subject to this Regulation in proper safeguarding procedures.

### D. PHYSICAL SAFEGUARDS

1. For all unclassified facilities, areas, and devices that process information subject to this Regulation, establish physical safeguards that protect the information against reasonably identifiable threats that could result in unauthorized access or alteration.

2. Develop access procedures for unclassified computer rooms, tape libraries, micrographic facilities, decollating shops, product distribution areas, or other direct support areas that process or contain personal information subject to this Regulation that control adequately access to these areas.

3. Safeguard on-line devices directly coupled to IT systems that contain or process information from systems of records to prevent unauthorized disclosure, use, or alteration.